



## WebSense Support Webinar: Questions and Answers

Creating custom policies and associating to directory objects  
WebSense Enterprise™ Version 6.3.x

**Question:** Is there a way to view exactly which clients have been assigned a specific policy?

**Answer:** Yes. Right-click on a policy in Websense Manager and select **View Assigned Clients**. This displays all clients that are assigned this policy.

**Question:** Can a **custom policy** be renamed?

**Answer:** Yes. Right-click on the policy and select **Rename**. Enter the new name. The same steps apply to renaming category sets and protocols.

The following cannot be renamed or deleted:

- \*Global Policy
- \*Always Block category set
- \*Default Settings category set
- \*Never Block category set
- \*Default Settings protocol set
- \*Never Block protocol set

The asterisk (\*) in front of the name indicates a policy or set that cannot be renamed or deleted.

**Question:** What is **password override**?

**Answer:** Password override lets users with valid passwords access Internet sites blocked by Websense software. Password override can be granted to clients (individual users, groups, workstations, or network ranges).

Select the target client, and check **Enable Password Override** at the top right of the screen. You are prompted to assign a password. When that client accesses a blocked site, a block page displays, with an option to type in the given password to view the page.

**Question:** Can **custom categories** be created under any category group?

**Answer:** Yes, custom categories can be created under any category group. Websense recommends creating all custom categories under the **User-Defined** category, for easy access and maintenance.

**Question:** Can specific URLs be used in multiple **yes lists**?

**Answer:** Yes. You can list the same URLs on multiple yes lists. Each yes list is unique and allows access only to the URLs it contains.



**Question:** When we created the **custom protocol set** during the Webinar, the Log option was selected for many of the items that were set to Block. Why do you need to log protocols, if they are already being blocked?

**Answer:** If you are blocking a protocol and would like to see which users attempt to use that protocol, select the Log option to see those attempts in your reports.

**Question:** Our Websense server is managed by an outside company, but I am responsible for my company's security. So, I would like to have read access to the rules. How can I accomplish that?

**Answer:** You have read and write permissions for all filtering policies if you are the **WebsenseAdministrator**. If you are not the WebsenseAdministrator, you can be granted these permissions via a feature known as **Delegated Administration**. (There is no specific option for read access only.)

To view or edit your policies, install Websense Manager on a workstation that is able to access your externally managed machine (the one that is running Websense Policy Server).

Option One: If the **WebsenseAdministrator** password is available to you, log on in Websense Manager using the default WebsenseAdministrator account. You can then view and edit all policies.

Option Two: If the password cannot be given to you, then your WebsenseAdministrator needs to add your domain account to the Super Administrator role. You need that specific role to be able to access all of the policies.

You would then be able to log on to Websense Manager with your domain credentials.

Adding your account to the Super Administrator role allows you to view and modify all of the filtering policies.

For details about the Delegated Administration feature, please see page 211 on the following Websense *Administrator's Guide*:  
<http://www.websense.com/SupportPortal/documents/v631/WSEAdminGuide.pdf>